Protecting Security Investment with Multi-Core Technology

February 2008

intel

NOKIA

In August 2006, Network World reported that attacks across Instant Messaging, chat, and peer-to-peer applications had grown an astonishing 700 percent compared to the previous year.[1]

Many threats are masquerading as legitimate application-layer traffic and getting past traditional firewall-based security appliances that focus on network layer access. Attacks are becoming more dynamic, which necessitates deeper packet inspection and preventative strategies across all network-layers. Combining expertise in security software, security appliances, and multi-core processors, three industry leaders are collaborating to develop a platform that applies leading-edge technologies to meet today's and tomorrow's security challenges.

Helping Keep Retail Safe

The Metro Group is an international retailer based in Germany with many well-known brands from supermarkets to electronics stores. Their infrastructure deploys more than 500 Nokia firewalls worldwide. Metro desired a centrally deployed firewall and selected Nokia IP2450 security platform because it offered a high-performance, scalable solution. Through its evaluation process, Metro found Nokia to focus on one technology, security appliances, which brought a better and deeper knowledge in this area than other vendors. They also appreciate participating in planning sessions and discussions around Nokia product roadmaps.

Evolving Security Attacks

Maintaining secure networks is one of the most challenging infrastructure problems facing governments, companies, and nearly every institution worldwide. And the reality is that security threats are evolving, increasing ain sophistication and attacking new vulnerabilities. This means security solutions must quickly bring new patches and policies online to safeguard the network.

Security threats are increasing at the application layer and exposing valuable information maintained by software such as financial, enterprise resource planning (ERP), and customer relationship management (CRM) systems. The application layer also supports many protocols that open the door to more access points and potential security breaches. When new application software is loaded onto network servers,
IT staff needs to be on the lookout for the introduction of new security holes.

To deal with new and ever-changing threats that appear with alarming regularity, security appliances must be flexible and able to handle new security attacks without degrading performance. "As threats become more sophisticated and as network traffic patterns change, security solutions must perform deeper inspections of more sizes and types of packets faster than ever before," says Tom Furlong, Senior Vice President, Connect, Communicate, Collaborate at Nokia.[2] Many traditional security devices are based on closed architecture and rely on ASICs and FPGAs to handle specific tasks very fast. But this approach, with security applications hard-coded in custom chips, can be poorly equipped to respond to dynamic threats.

Security appliances designed with open architectures, based on multi-core, high-performance processors, deliver the flexibility and performance needed to help protect against existing and potential threats. By combining the security and platform expertise of Nokia, Check Point, and Intel, institutions can deploy world-class security devices designed to meet next-generation security challenges.

> "The collaboration of Nokia, Check Point, and Intel offers a tighter integration of the hardware, operating environment and applications to allow customers to benefit from increased performance at decreasing prices."
>
> Andy Buss, Principal Analyst, Canalys[3]

Protecting Security Investment

Although every network is different, some security trends are likely to impact a majority of information and communication infrastructures.

- **Attacks occur on all layers of the network**
  In addition to firewalls that help protect connections (e.g., communications ports), security solutions require content-based protection that checks packet payloads carrying application-level data.
- **Packet payloads undergo more thorough stateful inspection**
  Next-generation security appliances require more computing performance to perform extensive pattern-matching routines used by intrusion inspection/detection applications.
- **Networks transition to 10 Gigabit Ethernet**
  Security infrastructure needs faster input/output to keep up with greater network traffic, which is fueling the adoption of faster networks.
- **IT increases intranet security infrastructure**
  In addition to perimeter defense, IT planners are increasing intranet infrastructure to help protect against threats that either originate or spread from within the institution. Typically, intranet network traffic exceeds internet traffic, and therefore necessitates a higher-capacity security appliance.

1. Gregg Keizer (Tech Message Corp.), "IM, P2P Attacks Up 700 Percent," Network World, 10 April 2006.
2. http://www.nokia.com/A4136001?newsid=946804
3. http://www.ebizq.net/news/8429.html

More robust security is required with the number of instances and severity of security threats growing at an alarming pace, as shown in Figure 1. "The most damaging and fast-moving threats today are content-based. Content-based attacks do not require sustained connections in order to do damage, and they almost always spread using connections that are inherently trusted. Being able to detect content-based threats effectively requires adequate processing power to support the security application," says Victoria Fodale, In-Stat industry analyst.

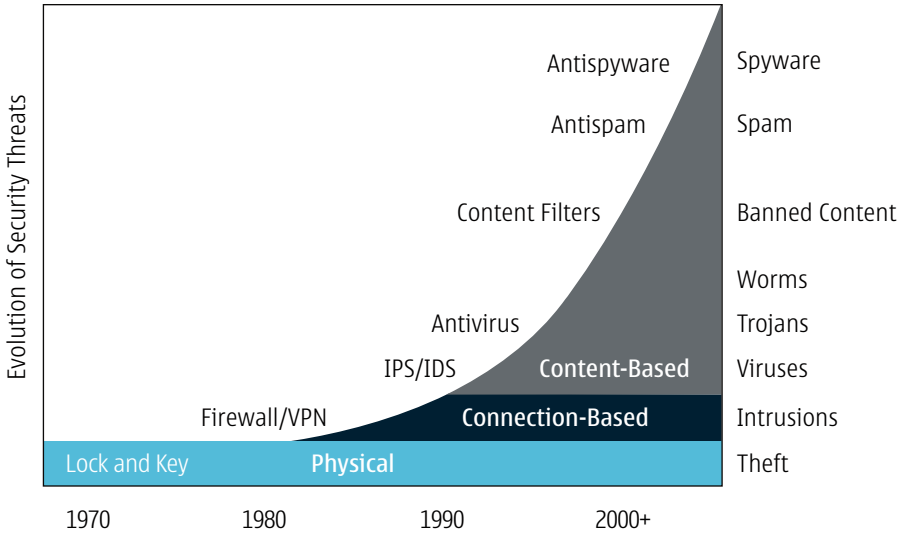

Figure 1: Evolution of security threats (copied with permission from In-Stat)

Maintaining System Value

Content-based attacks are dynamic, which can create some major issues for closed security systems dependent primarily on hardware acceleration. After their initial configuration, ASIC or FPGA-based systems cannot be reprogrammed to address new attacks. To combat these new attacks, closed systems often include a general-purpose (GP) processor that, through software updates, can close these security holes. This approach establishes two inspection tracks:

1. A fast path using hardware acceleration for simpler tasks
2. A slow path using a GP processor for more complex tasks often associated with web traffic, email, and VoIP

As a result, closed systems with hardware acceleration-based architectures may be particularly prone to decreasing performance as new attacks appear. Since the fast-path ASICs and FPGAs cannot be easily reprogrammed in the field to handle new threats, the GP processor deals with new attacks, which can make it run slower and slower over time.

The true value of a security system is its ability to deal with threats that have not yet appeared. Figure 2 illustrates two systems—one based on Check Point Open Performance Architecture and the other based on closed architecture—that start with equal performance values that later diverge as new attacks emerge. Over time, closed systems can lose their performance value. Open systems, based on multi-core processor designs, are programmable and can handle new situations with more predictable performance. This helps them to maintain and even increase their value to the network over the long run.

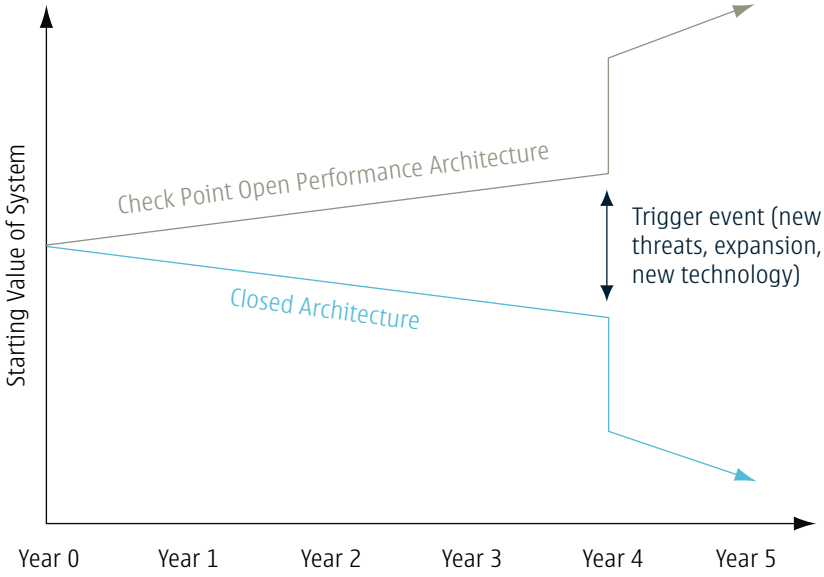

Figure 2: Security System Value Timeline[4]

4. Check Point white paper, "Delivering Application-Layer Security..."

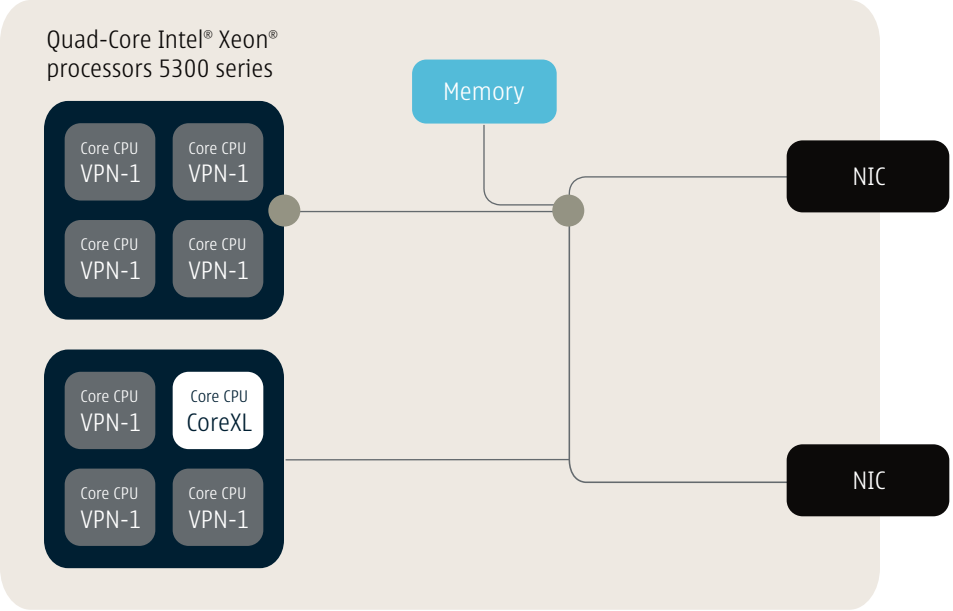

Figure 3: Check Point CoreXL Intelligently Balances Security Duties Across Multiple Cores

Combining leading-edge technologies

Nokia, Check Point, and Intel are sharing their respective expertise in appliance platforms, security software, and multi-core processors, enabling security solutions that have greater capacity to inspect network traffic in multigigabit environments.

Check Point CoreXL™: Multi-core Acceleration

Check Point CoreXL is based on security software technology that leverages multi-core processors and advanced load balancing to increase deep-packet inspection throughput needed for intrusion detection on the firewall. It works with VPN-1® Power™ Power Multi-core—an integrated firewall, VPN and intrusion prevention solution—and shares security inspection duties across available cores. Check Point CoreXL is a Check Point product and is not a member of the Intel® Core™ Duo processor family.

Using intelligence built into the director core, Check Point CoreXL distributes the load equally among the cores running Check Point VPN-1, as shown in Figure 3. Check Point CoreXL is designed to use as many cores as are available (4, 8, 16, and so on), enabling it to scale on higher capacity systems without changes. As new systems with more cores appear, VPN-1 Power Multi-core can be easily migrated—effectively enabling companies to gain more performance without changing solutions.

This load balancing technology prevents underutilized cores and suboptimal performance. The result is a 600 percent throughput increase when Check Point CoreXL is activated*. On a reference system using two 2.66 GHz Quad-Core Intel® Xeon® processors from the 5300 series, the throughput of integrated intrusion prevention increased from 300 Mbps to more than 1.8 Gbps* with over 70 percent of protections activated.

"Check Point VPN-1 Power Multi-core with Check Point CoreXL running on open multi-core architectures provides customers the flexibility to deal with new applications and threats while maintaining a predictably high level of performance. It is the only security solution in the market today that can fully leverage the performance benefits from multi-core architectures,"[5] says Dorit Dor, Vice President of Products at Check Point Software Technologies.

Check Point SecureXL™: Security Acceleration

Performance can be increased further using Check Point SecureXL, a software package with an API that can offload intensive security operations to a module specialized to handle them. This specialized module can be a third-party, dedicated hardware component or a performance-optimized software module. Check Point SecureXL helps accelerate firewall and VPN performance—such as throughput and connection rate—by offloading repetitive decisions from the general-purpose processor. It works in conjunction with Check Point CoreXL and multi-core platforms, like Nokia security appliances, by deploying a software-only upgrade or additional network processor hardware.

Nokia IPSO™: Hardened Operating System

Nokia security appliances run on an appliance-optimized, security-hardened operating system (OS) called Nokia IPSO. It supports VRRP/IP Clustering and key networking needs such as dynamic and multicast routing, IPv6, VLANs, link aggregation, and transparent mode, among many other features. And by using Nokia IPSO, system administrators can view detailed performance data across multiple CPU cores. Nokia IPSO has a robust toolset for administrators to manage Nokia IP security solutions using role-based administration via web-based Nokia Network Voyager interface or comprehensive Command Line Interface.

Nokia IPSO 6.0, the most recent release of the OS, is essential in leveraging multi-core technology in Nokia multi-core appliances, and a requirement to support Check Point CoreXL on Nokia security appliances. By combining multi-core technology and Nokia IPSO 6.0 with the capability to multi-thread, new security applications such as Check Point CoreXL can efficiently maximize the use of Nokia IPSO and the appliance processors to achieve better responsiveness, minimize blocking problems, and gain better performance. By splitting the work among multiple cores, multi-core appliances running Nokia IPSO can simply perform more work per unit of time.

Quad-Core Intel Xeon Processors: Multi-core Computing Platforms

Security systems running on eight CPU cores, supplied by two Quad-Core Intel Xeon processors from the 5300 series, are providing the performance headroom needed to help protect networks into the future. Based on the Intel Core microarchitecture, these processors offer breakthrough performance—up to three times the raw performance and performance/watt* of previous-generation single-core processors. This translates into greater performance with fewer cooling challenges and enables security applications to run

5. http://www.checkpoint.com/press/2007/security-acceleration-technology053007.html

within a smaller footprint.

Delivering Performance Over the Solution's Lifetime

Institutions worldwide are looking for security appliances that help protect both their networks and infrastructure investments. This requires platforms that can adapt to changing network traffic and threats, thereby avoiding costly hardware forklift upgrades.

To support future needs, custom-built security hardware architecture incorporates unique features—such as expanded bus lanes, multigenerational interface support, and Accelerated Data Path (ADP) add-in card technology—that essentially creates an "appliance within an appliance." Nokia IP2450 security platform can be upgraded to more than double firewall throughput (approximately 9 to 20 gigabits) through optional ADP cards that leverage Check Point SecureXL software. Nokia ADP cards are available with 12 ports of Gigabit Ethernet in 1000Base-T as well as 12 ports of Gigabit Ethernet in 1000Base-X with interchangeable small form-factor pluggable (SFP) modules supporting SX, LX, and copper interfaces. This flexibility allows IT to expand capacity and performance as needs grow.

In addition to raw security performance, IT professionals are looking for solutions that are compact, reliable, and cost-effective. With a space-saving two rack unit (2RU) form factor, Nokia IP2450 security platform offers the smallest form factor using a non-bladed appliance approach, which helps to avoid a costly up-front chassis investment. It incorporates High Availability features such as redundant hot-swappable power supplies, hot-swappable fan trays, and optional redundant hard disk drives with RAID 1.

Providing Best-In-Class Value

Many businesses face unpredictable growth from mergers, acquisitions, or other business changes, which places higher performance demands on their network security appliances. Nokia, Check Point, and Intel are combining their software, hardware, and platform technologies and enabling more flexible and agile solutions that can help companies better protect their networks from attack while preserving their infrastructure investment. Intel multi-core processors running Check Point software are integrated into a solution from Nokia that delivers tuned performance and investment protection backed by global technical support.

"Combining security software with open systems running general-purpose processors allows customers to benefit from rapid performance improvements coming from the world's leading chip manufacturer," adds Dorit Dor of Check Point.

One of the first solutions is Nokia IP2450, a high-end, next-generation security appliance designed for the demanding price performance and Multigigabit Ethernet throughput requirements of large businesses and service providers. It offers the smallest form factor, lowest price per port, and lowest price per gigabit of firewall throughput in its class. This "greener" approach—increasing performance without increasing footprint—helps make better use of data center space.

For more information, please visit: usa.nokia.com/business

Terms

API (application programming interface): a specification that standardizes the method by which a program communicates with another program.

ASIC (application-specific integrated circuit): a custom chip that is designed for a specific application rather than a wide variety of software.

CRM (customer relationship management): a set of tools used to interact directly with customers.

ERP (enterprise resource planning): business software used to run various aspects of a company, including managing orders, inventory, and accounting.

FPGA (field-programmable gate array): a chip composed of an array of configurable logic cells that can be configured, or programmed, to perform a specific function.

IP Clustering (Internet Protocol Clustering): a technology that allows several independent appliances to join together for a common security goal as one virtual machine.

* Performance tests and ratings are measured using specific computer systems and/or components and reflect approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit www.intel.com/performance/resources/benchmark_limitations.htm.

About Nokia

Nokia is the world leader in mobile communications, driving the growth and sustainability of the broader mobility industry. Nokia is dedicated to enhancing people's lives and productivity by providing easy-to-use and secure products like mobile devices, and solutions for imaging, games, media, mobile network operators, and businesses. Nokia is a broadly held company with listings on five major exchanges.

For more information, please visit:
www.nokiaforbusiness.com

About Intel

Intel, the world leader in silicon innovation, develops technologies, products, and initiatives to continually advance how people work and live. Additional information about Intel is available at www.intel.com/pressroom and blogs.intel.com.

For more information, please visit:
www.intel.com

Work together. Smarter.

Nokia Inc. 102 Corporate Park Drive, White Plains, NY 10604 USA • www.nokiaforbusiness.com
Americas Tel: 1 877 997 9199 • Email: usa@nokiaforbusiness.com
Asia Pacific Tel: +65 6588 3364 • Email: asia@nokiaforbusiness.com
Europe, Middle East, and Africa France +33 170 708 166 • UK +44 161 601 8908 • Email: europe@nokiaforbusiness.com

Intel Corporation 2200 Mission College Blvd., Santa Clara, CA 95054 USA • www.intel.com
Worldwide Tel: 1 408 765 8080